Wireshark

So now that you have entered a network and intercepted the traffic it is time to analyze that traffic. That can be with wireshark.

Filters

There are two types of filters that we can use. 1. Capture filter - This filters out in the capture process, so that it does not capture what you have not specified. 2. Display filter - This filter just filters what you see. You might have captured 1000 packets, but using the display filter you will only be shown say 100 packets that are relevant to you.

The syntax for the two filters are a bit different.

Capture filter

So if you just start capturing all traffic on a network you are soon going to get stuck with a ton of packets. Too many! So we might need to refine out capture.

Click on the fourth icon from the left. If you hover over it it says `Capture options`

Some useful might be. From a specific host and with a specific port:

```
host 192.168.1.102
port 110
```

Display filter

Show only packets used by this IP-address, or to a specific port

```
ip.addr == 192.168.1.102
tcp.port eq 25
```

Automatically resolve ip-addresses

Easy https://ask.wireshark.org/questions/37680/can-wireshark-automatically-resolve-the-ip-address-into-host-names